A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2002-1129-4T

INDEPENDENT STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE
COMMISSION ON JUDICIAL CONDUCT

July 1, 2000 Through December 17, 2001

OFFICIAL AUDIT REPORT
APRIL 12, 2002

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Commission on Judicial Conduct (MCJC) is a state agency which, under its enabling statute Massachusetts General Law Chapter 211C, is responsible for investigating complaints of judicial misconduct against state court judges and for recommending to the Supreme Judicial Court disciplinary action of judges, when necessary. All fifty states and the District of Columbia have judicial conduct agencies to investigate allegations of judicial misconduct and disability that would prevent judges from properly performing their judicial duties. The MCJC is responsible to preserve both judicial independence and public accountability. The Commission serves to maintain the public's confidence in the integrity of the judicial system by providing a fair and reasonable process to address judicial misconduct and disability.

The Commission consists of nine members: three judges appointed by the justices of the Supreme Judicial Court, three members of the bar appointed by the chief administrative justice of the trial court, and three members appointed by the governor. An executive director oversees the daily administrative operations of the Commission with a staff of five employees. The Commission's information technology infrastructure consists primarily of a Microsoft NT Local Area Network (LAN), which is operating through the support of a third-party consultant.

In accordance with its responsibilities to be able to conduct an investigation with complete accountability, impartiality, and strict confidentiality, the MCJC must maintain absolute security in its daily operations with respect to the systems of record for investigative files, paper files, and its electronic data base. It is therefore important that the LAN be maintained at a high level of security and accountability according to good general business practices and in accordance with Massachusetts General Laws. The MCJC does not have the authority to order a judge to step down from hearing a case or to provide a complainant with a different judge. The Commission does not serve as an appellate court to review judges' rulings, and therefore cannot review, reverse, or vacate a judge's decision.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From October 25, 2001 to December 17, 2001, we performed an information technology (IT) audit at the Massachusetts Commissioner on Judicial Conduct (MCJC) covering the period of July 1, 2000 through December 17, 2001. Our audit scope included an examination of internal controls over selected information technology functions pertaining to physical security, environmental protection, logical access security, hardware inventory, disaster recovery and business continuity planning, and on-site and off-site storage of backup magnetic media.

Audit Objectives

The primary objective of our audit was to determine whether adequate controls were in place and in effect to provide a properly-controlled IT environment. We determined whether adequate controls regarding physical security and environmental protection were in place and in effect to safeguard computer operations and IT-related assets. With respect to access security, we sought to determine whether adequate controls were in place to prevent unauthorized access to system and application software and related data files residing on the Commission's LAN-based file servers and desktop computers. Our objective with respect to inventory control was to determine whether computer equipment was properly identified, recorded, and accounted for in the Commission's inventory system of record.

With respect to the availability of automated processing capabilities and access to electronic information resources, we determined whether disaster recovery and business continuity controls were in place to provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems be rendered inoperable or inaccessible. In conjunction with reviewing business continuity planning, we determined whether proper backup procedures were being performed and whether copies of backup magnetic media were stored in secure on-site and off-site locations.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding MCJC's overall mission and its IT environment. The pre-audit work included interviews with senior management, a review of policies, procedures, and other internal control documentation, and observation of IT-related areas. To obtain an understanding of the Commission's activities and

internal control environment, we reviewed MCJC's mission, organizational structure, and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To determine whether IT-related assets were adequately safeguarded, we reviewed physical security and environmental protection over the LAN file servers and desktop computers through observation, interviews with MCJC management and staff, documentation review, and completion of appropriate audit checklists.

We reviewed MCJC's logical access security policies and procedures to prevent unauthorized access to the MCJC software and data files residing on the Commission's LAN and work stations. We reviewed the security policies and procedures with the Executive Assistant who was responsible for controlling MCJC's access to the Commission's LAN and desktop computers. Since the MCJC uses the Windows NT operating system to control access to its Local Area Network (LAN), we reviewed the installed network security policy as maintained by NT for adherence to generally accepted security practices. Specifically we reviewed the secure settings for password length, password expiration, and password history. As part of our examination of logical access security, we determined whether users having active user accounts were authorized to have access and were current employees of the Commission. We determined whether individuals granted access to the Commission's systems were currently employed by the Commission by comparing an automated list of individuals authorized to access the system with an official listing of current employees. In addition, we determined whether all system users were required to change their passwords periodically and, if so, whether the frequency of password changes was appropriate. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed procedures for authorizing access to and deactivating access from MCJC's IT resources on the LAN and desktop computers.

To determine whether IT resources were properly accounted for, we reviewed inventory policies and procedures, interviewed appropriate staff, and examined the Commission's system of record for maintaining an inventory of equipment. To determine whether the MCJC's hardware inventory record was accurate, complete, current, and valid, we reviewed inventory data for 33 items (100%) of computer and related equipment located at the MCJC. Moreover, to determine whether all items of computer hardware that were physically located at MCJC were listed on the inventory record, we traced selected items to the inventory records. Further, to test whether purchased items of hardware were being listed on the system-of-record for inventory and

physically located at the MCJC, we compared purchase orders and invoices for the two items of hardware purchased by the MCJC during fiscal year 2001 to the inventory records and located the individual software items at the MCJC offices. We also determined whether computer equipment was properly inventoried and verified the serial numbers to the inventory record.

To assess the adequacy of disaster recovery and business continuity planning, we reviewed the level of planning and established procedures to be followed to resume computer operations in the event that the file server and desktop computers were rendered inoperable or inaccessible. We interviewed MCJC management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been identified and evaluated, whether a written business continuity plan was in place, and, if so, adequately tested. The interview also addressed an evaluation of the adequacy of controls to ensure that software and data files would be available for recovery efforts should the automated systems be rendered inoperable. The software availability review addressed the adequacy of provisions for on-site and off-site storage of critical backup tapes. In that regard, we interviewed MCJC staff responsible for creating and storing backup copies of computer-related media.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted auditing practices. Audit criteria used in the audit included management policies and procedures, and control guidelines outlined in *Control Objectives for Information and Related Technology* (CobiT) as issued by the Information Systems Audit and Control Association, July 2000. CobiT's control objectives and management control guidelines provide generally applicable and accepted standards for sound information technology security and control practices that serve as a framework for control reference for management, users, security practitioners, and auditors.

AUDIT SUMMARY

Based on our audit, we found that information technology-related controls in place at the Massachusetts Commission on Judicial Conduct provided reasonable assurance that the Commission's computer equipment was properly accounted for and was operating in a properly-controlled environment. Internal controls, however, needed to be strengthened to provide reasonable assurance that control objectives regarding physical and logical security and business continuity planning would be met.

We found that the Commission had appropriate controls in place to provide reasonable assurance that IT resources would be properly accounted for on the Commission's system-of-record for its equipment inventory. Our audit tests indicated that the inventory system-of-record was accurate, complete, current, and valid for computer equipment. We also found that computer equipment recorded on the inventory could be located and was found to be properly tagged. In addition, computer equipment purchased within the past year was found to be properly recorded on the inventory record and could be readily located at the Commission's office location.

Our audit revealed that adequate environmental protection was being provided for the MCJC's IT-related assets. In this regard, we found that the areas housing computer equipment were well maintained with an appropriate level of housekeeping, appropriate air quality was being afforded to the file server room, a fire emergency plan was in place and posted, and there were fire detection and fire alarm devices installed and fire suppression controls in place.

We found that less than adequate physical security was being provided to protect IT resources, since the Commission's office area was not alarmed to help guard against unauthorized access, damage or theft. Although adequate compensating controls appear to be in place to support physical security, overall, we believe that the Commission would benefit from strengthening controls to prevent unauthorized access to the office areas. We recommend that the Commission consider using a magnetic card system, or key punch code system, because these systems offer a higher level of control for different levels of access over a key-based system. We found that the office area was not intrusion alarmed, which would leave the entire office and computer area vulnerable to undetected intrusion.

Regarding logical access security, although the Commission required system users to sign a pledge to maintain confidentiality the form did not sufficiently address appropriate strictures for computer use. While the current form helps ensure that users understand their responsibilities regarding information contained within hardcopy records, it does not sufficiently address IT-

related security. Our examination of access privileges indicated that individuals having access had been authorized to use the Commission's computer systems, but that controls to ensure that access privileges were deactivated in a timely fashion for users no longer authorized or needing access. Our review of authorized access accounts for users compared to a recent list of current employees found that there were user accounts that had not been deactivated for three individuals who were no longer employed at the Commission. Also, there was an absence of control procedures, including written policies and procedures regarding password formation and use, periodic change of passwords, and deactivation of logon ID's and passwords when an employee's status changes.

Regarding operating system security, we found that, contrary to sound IT security directives, the Commission had allowed default settings within the NT operating system of "no password", "no password length", "no password age" and "no account lockout" on the account policy of users. The failure to properly set these parameters hinders the ability of the Commission to enforce good security practices and increases the risk of unauthorized access. Poor, or inappropriate password security settings may allow unauthorized users to access to the system. In addition, the failure to deactivate logon IDs and passwords may also allow unauthorized access to confidential client information, because the access privileges may continue to be available for use of staff who have terminated or transferred employment. Generally accepted computer industry standards indicate the need to prevent and detect unauthorized system access through the implementation of formal control procedures for logical access security. Failure to implement adequate controls concerning access security could result in unauthorized system access or use.

With regard to the continued availability of computer operations and access to electronic information, we found that disaster recovery and business continuity plans needed to be strengthened. Regarding recovery strategies and contingency plans, we found that the Commission did not have a formal, tested business continuity plan that would be used for the timely restoration of business functions provided by automated systems should IT resources be rendered inoperable. In addition, although the Commission generated and stored backup copies of magnetic media at an on-site location, backup copies were not stored at an off-site location. Without off-site storage of backup media and sufficient business continuity planning, including a viable alternate-processing site, a possible long-term loss of the MCJC's computer operations could hinder access to processing capabilities and electronic information needed to perform business functions. We recommend that the Commission implement off-site storage procedures for backup copies of magnetic media.

We recommend that the Commission assess the relative criticality of its automated systems and conduct a formal risk analysis of its IT components, including outsourced services. Based on the results of the criticality assessment and risk analysis, the Commission should confirm its understanding of business continuity requirements and, as necessary, amend recovery plans to address mission-critical and essential IT-supported business functions and services.

AUDIT RESULTS

1. Physical Security

We found that the physical security over the general office area, the designated computer room, and the confidential records room needed to be strengthened. We determined that although the front door to the Commission was kept locked at all times, the lock mechanism was a standard lock and key rather than a magnetic card or punch keypad. The use of hard key access system rendered the office easily accessible by potential duplicate keys. Magnetic and keypunch locks can have access combinations changed easier than a key lock which would facilitate combination changes in order to improve security.

We determined that the room used to store confidential records also had a lock and key rather than a magnetic card or punch keypad system. The key used to access the confidential records room was different than the key used to access the front door and was restricted to fewer staff. During office hours, however, unlike the office's front door, the doors to the confidential records room were left open. Since the records kept in this room do not have off-site backup and are in some instances unique, a greater level of care must be employed to safeguard these records. We noted that there was no intrusion detection alarm system for the office area, computer room, or confidential records room. There was also a large unalarmed window with the potential for unauthorized access.

Generally accepted security practices require that adequate preventive and detective physical access security controls are in effect to ensure that only authorized access can be obtained. Failure to effectively secure facilities could result in the theft or destruction of resources, IT equipment, and disruptions or loss of IT services any of which could halt or disrupt mission-critical business objectives.

Recommendation:

We recommend that MCJC install alarms on exterior windows and doors to detect and to initiate notification of unauthorized entry. We suggest that the alarm system be configured so that in the event of an unauthorized access attempts, in addition to a sonic alarm, the alarm system should also notify selected staff or security personnel for follow-up action. Additionally, the management team at MCJC should consider changing the key lock system to a magnetic pass card, or punch pad system. We also recommend that should the confidential records room's key-lock be changed to a magnetic card or punch keypad, a different access code should be used

instead of the code used for the entrance door to established security zones to restrict access to only designated employees.

Auditee's Response:

> *Alarming of office area and windows; magnetic card system or key punch for entry and file room. It is the intention of the Commission that our offices will be moved to a new location as of October 1, 2002, when our lease here ends. As we have no money to spare in our budget and will be lucky to cover regular operating expenses, it would not be wise for us to spend the money to change these systems in this office for the few months we expect to remain here. We have requested that the Division of Capital Asset Management (DCAM) include a magnetic card system in the request for proposal (RFP) that will issue for the Commission's new office space.*

Auditor's Reply:

Although we concur with the Commission 's intent to alarm their new offices when they move to a new location as of October 1, 2002, we remain concerned that the MCJC will be left vulnerable over the next six months until this alarming can occur. We recommend that the Commission consider using a portable motion sensor/alarm system in the current location that may be able to be used in their new location.

2. Logical Access Security Administration

Our audit disclosed that although certain system access security controls were in place, other control procedures needed to be strengthened to ensure that only authorized users have access to IT resources at MCJC.

Although MCJC is a small agency with a staff of five employees, we found that appropriate procedures were in place to authorize access to computer systems and to activate user logon ID and password accounts. We found, however, that procedures to deactivate access privileges needed to be strengthened to ensure that user accounts were not left active for individuals no longer requiring or authorized to have access privileges. Current procedures did not provide reasonable assurance that access privileges would be deactivated for users no longer authorized or needing access to the automated systems. As a result, we found that logon IDs and passwords were left active for three individuals no longer authorized or needing access to the system. Failure to deactivate logon IDs and passwords may allow unauthorized access to confidential client information since the access privileges of staff that have terminated or transferred employment, or taken new positions within the Commission, may continue to be inappropriately available for use. Changes in employment status that should affect system access privileges are:

termination of employment, change of position or job responsibilities that impact the level of access required, and extended leaves of absence when access is not required.

When the MCJC installed the Windows NT operating system on its local area network the system administrators neglected to set security restrictions in accordance with generally accepted security practices. By allowing the initially blank default security settings, or parameters, to remain after the installation of NT, rather than establishing secure settings for password length, password expiration, and password history, MCJC's installed network security policy did not verify the length of a user's password, specify when a password would expire, or check to see whether a password had been used before. Under these circumstances, when asked to establish a password by the NT system, a user could have responded by hitting the "enter key" and thus have no password or in other words a password with a length of zero characters. Generally accepted computer industry standards and practices for sound password administration require a password with a length of at least eight characters. Also, a common practice is to require the use of alphanumeric passwords, which specifies the use of numbers and letters in the password to increase the difficulty of guessing someone's password. Understandably, the strength of the password can be further enhanced by using special or foreign language characters. Because the system's parameters had not been set to require that passwords expire on the MCJC system, the user could keep the same password indefinitely. If at some future date a user were asked to create a new password, and if the security settings were not changed, the user could re-use the same password, or "enter key" and thus repeat having no password, since a history of prior used passwords was not being maintained.

We verified the list of active system users with a recent payroll list of employees and determined that there were three users who maintained access permissions although they were no longer employed by the Commission. Through interview with the system administrator, we determined that there was no policy or procedure to remove status-changed employees from the LAN in a timely manner.

Generally accepted computer industry standards indicate the need to prevent and detect unauthorized system access through the implementation of formal control procedures for logical access security. The control procedures should include written policies and procedures regarding password formation and use, required periodic changes of passwords, and formal procedures to deactivate logon IDs and passwords when an employee's status changes. Failure to implement adequate controls regarding logical access security could result in unauthorized system access that could thereby result in unauthorized disclosure or use of confidential information or alteration of data.

The access security problems identified by our audit may have occurred because the system administrator at MCJC is a consultant who was not located on the premises of the MCJC. By the end of the audit, the MCJC had removed the three former staff members from the users list.

Recommendation:

We recommend that the Commission modify the NT security settings for the LAN to increase access security control as soon as possible. Appropriate security parameters need to be set for use of required password, password length, password expiration, frequency of password changes, password composition, and password history. We further recommend that security settings be reviewed at least twice a year if not more frequently. We recommend that the Commission modify their current confidentiality form to include electronic documents and logical access security requirements. The latter should outline appropriate password practices such as maintaining the confidentiality of their password and commitment to protect the password from unauthorized use and/or disclosure.

We further recommend that documented practices regarding authorization, password length, password expiration and password history be included in the Commission's internal control plan as required by Chapter 647 of the Acts of 1989 and the Office of the State Comptroller. Policies and procedures should also include procedures for deactivation and deletion of logon IDs and passwords. We also recommend that MCJC implement policies and procedures to help ensure that the security administrator is notified in a timely manner of changes in employee status, such as terminations, extended leaves of absence, employee transfers, and inter-departmental changes in authorization levels. Once notified of the change in employment status, the security administrator should deactivate and/or delete the logon ID and password in a timely manner. Appropriate staff members should be instructed regarding adherence to policies and procedures.

We also recommend that MCJC modify access security controls to ensure that access privileges would be deactivated after an established period of inactivity. We recommend that the system administrator monitor the appropriateness of users assigned access to the automated systems, and deactivate logon IDs and passwords for users no longer needing access to the system. We also recommend that the internal control plan address security violations, monitoring and reporting of access attempts, and follow-up procedures for violations and violation attempts.

Auditee's Response:

> *The Oath of Confidentiality which we showed your auditors at their request was just a draft which the Commission was considering. The Commission had*

deferred action on this matter, and no oath has ever been required in writing. I will implement a requirement that each staff member sign an oath of confidentiality which will include electronic documents and passwords.

Our Executive Assistant will see to it that our consultant fixes the deficiencies in our NT security settings for the LAN within two weeks of this date. Our Executive Assistant will also create written policies and procedures for the formation, use and change of passwords.

Access being obtained by users no longer authorized was not a worry to us, as anyone no longer authorized to use the system is not authorized to be in the office unsupervised. Nevertheless, we understand the need to immediately deactivate the access of any such persons in the future and will do so. There is no such thing as "employee transfer" or "interdepartmental changes" in our office of five people.

Auditor's Reply:

We agree with your plans to have MCJC staff sign an oath of confidentiality, which will include electronic documents and passwords. We acknowledge that it is unlikely there would be security risks based on interdepartmental transfers given the size of the Commission, but rather that a reassignment of responsibilities may warrant a change in user access privileges. Until the deficiencies in the NT security settings are rectified for the LAN an adequate level of security is not in place. We are pleased that the Commission is taking corrective action on addressing the NT security settings. We suggest that the policies and procedures being documented for the formation, use, and change of passwords also include a requirement for periodic review of the NT security settings. We will review the logical access security settings at our next audit.

3. Business Continuity Planning

We determined that, as of the start of our audit, the Commission did not have a documented business continuity plan to provide for the timely restoration of mission-critical and essential business functions should systems that are processed through its local area network be rendered inoperable. Although we found that MCJC was performing backup procedures for applications residing on its LAN, and was backing up MCJC data files to tape, there was no off-site tape storage of these backup media. MCJC had not designated or tested an alternate-processing site to be used in the event a disaster occurs.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for

computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. To that end, MCJC should assess the extent to which the Commission is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical requirements of its information systems.

The assessment of impact should identify the extent to which Commission's business objectives and functions are affected over various time frames of the loss of processing capabilities. The assessment of criticality and impact of loss of processing should assist the Commission in triaging its business continuity planning and recovery efforts.

By the end of our audit field work, MCJC had developed a one-page business continuity strategy and had drafted a memorandum of agreement with a another state agency to serve as the possible location for off-site storage and as an alternative processing site from which to perform a disaster recovery operation. However, the absence of a formal, tested business continuity plan, and alternate processing agreement places at risk the Commission's ability to regain mission-critical and essential data processing operations that support administrative functions within an acceptable time period. The Commission's efforts to ensure that backup copies of data files and programs are being stored on and off site is a good first step in addressing the requirements for viable business continuity planning.

Recommendation:

The MCJC should immediately establish off-site storage for backup copies of magnetic media. In addition, the MCJC should establish a business continuity-planning framework that incorporates criticality and impact assessments, risk management, business continuity plan development, recovery plan testing and maintenance, training, and communication. Disaster recovery procedures should be developed to ensure that the relative importance of the Commission's systems is evaluated on an annual basis, or upon major changes to the IT infrastructure, application systems, or user requirements. The MCJC should also conduct a formal risk analysis of its IT-related components on an annual basis, or upon major changes to the relevant IT infrastructure, or to business operations or priorities.

Auditee's Response:

> *Our Executive Assistant will make sure that our written plans for disaster recovery and business continuity meet your requirements, and he will begin offsite storage as required.*

Auditor's Reply:

We would like to reiterate that implementation of off-site storage of backup media is a critical first step in addressing business continuity planning. Since business continuity requirements are based upon the need for the availability of electronic information and IT processing, the Commission should consider triaging their efforts to address critical information and processing needs first. Understandably, the development of a viable business continuity plan includes access to IT resources and having an alternate site available from which the Commission's operations can continue. In addition, factors to be considered would be identified through a risk assessment of the Commission's IT infrastructure and operating environment. We will review the revised written plans for disaster recovery and business continuity at our next audit.